2.4. Preparation for Post-Quantum Cryptography

Objective

2.4.1. Agencies are prepared for the impacts that widespread availability of quantum computing will have on information security.

Context

Scope

2.4.2. This section provides information for agencies to assist with preparation for the impacts of quantum computing on information security, and more specifically impacts related to encryption.

Background

2.4.3. There has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. The pace of this research is accelerating.

2.4.4. The development of quantum computing is a rapidly advancing area with multiple innovations being announced regularly, often eclipsing previous forecasts.

2.4.5. Quantum computers are not expected to fully replace classical computers as quantum effects are currently useful only on particular tasks. However quantum computers will be able to rapidly solve highly complex problems, well beyond the capabilities of today's supercomputers.

2.4.6. A prominent area of quantum computing applicability is in the field of cryptanalysis, and it is expected that they will be able to compromise or render ineffective many of the public-key cryptosystems currently in use.

2.4.7. It is important that agencies are aware of the potential impact developments in quantum computing are likely to have on critical security controls such as encryption. It is also important that they are preparing to act to minimise the disruptions that could be caused during migrations to post-quantum cryptography (cryptographic systems that remain secure after the widespread availability of quantum computing).

2.4.8. Currently there are no post-quantum cryptographic systems approved for use in the NZISM, however there are actions that agencies can undertake to prepare for the time when such systems are approved.

Post-Quantum Cryptographic Standards

2.4.9. International organisations are evaluating potential candidates for standardisation in post-quantum cryptography. GCSB will review applicable standards and consider them for incorporation into the NZISM when they are published.

2.4.10. When standards for quantum-resistant public key cryptography become available, GCSB may deprecate or withdraw support for existing classical cryptographic standards. Agencies should therefore be prepared to transition away from these algorithms possibly in the next 2-3 years, even though the standards to migrate to are still to be developed.

2.4.11. Until new quantum-resistant algorithms are standardised, agencies should maintain or strengthen their existing cryptographic position using the algorithms, protocols and key lengths specified in Chapter 17 - Cryptography.

References

2.4.12. Additional guidance on post-quantum cryptography can be found at:

Reference	Title	Publisher	Source
	Getting Ready for Post-Quantum Cryptography	NIST National Institute for Standards and Technology	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf [PDF, 401 KB]
	Post-Quantum Cryptography Project (NIST)	NIST National Institute for Standards and Technology	https://csrc.nist.gov/projects/post-quantum-cryptography
	Post-Quantum Cryptography	Department of Homeland Security (US DHS)	https://dhs.gov/quantum
	Migration To Post-Quantum Cryptography	National Cybersecurity Center of Excellence (US NCCoE)	https://nccoe.nist.gov/sites/default/files/library/project-descriptions/pqc-migration-project-description-final.pdf [PDF, 386 KB]

Rationale & Controls

Post-Quantum Cryptography Preparation

2.4.13.R.01. **Rationale**

International organisations are in the process of developing standards for post-quantum cryptographic algorithms. The standards will be reviewed and incorporated into the NZISM as they are published.

2.4.13.R.02. **Rationale**

As standards are still under development the form of post-quantum cryptography is not fully determined at this point in time.

2.4.13.R.03. **Rationale**

It is recognised that providing guidance on the concrete and achievable steps that can be taken now to prepare for the transition to post-quantum cryptography will help ensure a smooth and efficient transition to any new standards that become available.

2.4.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7206]

Agencies SHOULD ensure they are aware of the latest developments in post-quantum cryptography. GCSB is tracking these developments and will continue to provide advice through the NZISM.

2.4.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7207]

Agencies SHOULD maintain an inventory of sensitive and critical datasets that must be secured for an extended amount of time. This will ensure datasets that may be at risk now and decrypted once a cryptographically relevant quantum computer is available are not secured solely through the use of quantum vulnerable cryptography.

2.4.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7208]

Agencies SHOULD conduct an inventory of systems using cryptographic technologies to determine the potential size and scope of future transition work once post-quantum cryptographic systems become available.

2.4.13.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7209]

Agencies SHOULD identify which systems in their inventory rely on public key cryptography and note them as quantum vulnerable in agency risk assessments.

2.4.13.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7210]

Agencies SHOULD determine a priority order for quantum vulnerable systems to be transitioned from classical cryptography to post-quantum cryptography.

2.4.13.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7211]

Agencies SHOULD consider the following factors when prioritising the quantum vulnerable systems:

- Is the system a high value asset based on agency requirements?
- Does the system protect sensitive information (e.g., key stores, passwords, root keys, signing keys, personal information, and classified

information)?

- Do other systems (internal or external to the agency) depend on the cryptographic protections in place on the quantum vulnerable system?
- How long does the data need to be protected?

2.4.13.C.07. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7212]

Using the inventory and prioritisation information, agencies SHOULD develop a plan for system transitions upon publication of the new post-quantum cryptographic standard.